

Lettre des "Lundi de la cybersécurité n° 60

Analyse de l'état de la cybermenace - Retour sur 1 an de conflit Russo- Ukrainien

Par webinaire Zoom
et en présentiel à l'université Paris Cité
si le nombre d'inscrits en présentiel le
justifie



Lundi 12 juin
18h00-20h00



Analyse de l'état de la cyber-menace
Retour sur 1 an de conflit Russo-Ukrainien



Ivan Fontarensky
Directeur technique
Lutte Informatique Défensive
Thales

Organisateurs



Pr Ahmed Mehaoua
Université Paris Cité



Béatrice Laurent



Gérard Peliks

Analyse de l'état de la cybermenace Retour sur 1 an de conflit Russo-Ukrainien

Le cyberspace, le numérique, l'Internet, autant de mots devenus familiers et qui décrivent un monde dans lequel nous vivons aujourd'hui. L'information recherchée, où qu'elle soit, est à portée de clics, nos correspondants où qu'ils se trouvent sont accessibles par mail ou par les réseaux sociaux, Internet ne connaît pas de frontières et le monde numérique est un village global où les distances n'existent pas. C'est merveilleux...

Mais...

L'Internet est aussi le carrefour de tous les dangers, le cyberspace est peuplé d'individus peu recommandables, qui vous rançonnent ou chiffrent ou détruisent vos données. Internet est un champion de la conflictualité, il est peuplé de pays qui ne nous

veulent pas du bien, ou qui sont en concurrence économique avec nous. Les applications que nous utilisons, et dont nous dépendons, présentent des vulnérabilités par lesquelles les cyberattaquants s'engouffrent et se retrouvent dans vos systèmes d'information.

Et quand deux pays sont en état de guerre et que ce conflit peut s'étendre, les cyberattaques ne concernent pas que ces pays. Tous, nous sommes menacés, nous sommes en état de cyberguerre. Le conflit Russo-Ukrainien nous concerne, nous menace et les cyber attaques, orchestrées en particulier par les Russes et leurs affiliés hacktivistes, contre nos informations, se multiplient.

Alors, comprendre et analyser le niveau des menaces cyber qui nous entourent, connaître les modes opératoires des attaquants, pour adapter sa ligne de défense, sont une nécessité mais qui demandent des connaissances techniques pointues, c'est une affaire d'experts et d'outils adaptés.

Pour nous éclairer, dans ce lundi de la cybersécurité du mois de juin, nous faisons appel au **directeur technique « Lutte Informatique Défensive »** de chez **Thales**, un expert reconnu de la **Cyber Threat Intelligence**, ou renseignement d'intérêt cyber : **Ivan Fontarensky**.

Ivan prendra comme exemple le conflit entre la Russie et l'Ukraine, un conflit qui nous concerne tous. Il est à noter que l'Ukraine est devenue, très récemment, membre du Centre d'excellence de l'OTAN pour la cyberdéfense coopérative (CCDCOE).

J'ai eu le privilège de travailler avec Ivan quand nous étions chez Airbus Cybersecurity, ses présentations m'ont toujours passionné. Les années ont passé et Ivan est très écouté dans la sphère de la cyberdéfense. J'ai tenu à vous en faire profiter.

Je donne la plume à Ivan Fontarensky

Une nouvelle cartographie des attaques se profile après douze mois de conflit. Alors qu'au moment de l'invasion, la majorité des incidents dans le monde se concentre en Ukraine (50,4% au premier trimestre 2022 contre 28,6% au troisième trimestre), les pays membres de l'Union européenne ont connu une augmentation spectaculaire du nombre d'attaques liées au conflit au cours des six derniers mois de l'année 2022, passant de 9,8% à 46,5% des attaques mondiales.

Pendant l'été, le nombre d'incidents liés au conflit dans les pays de l'UE était comparable à celui de l'Ukraine (85 contre 86). Le début de l'année 2023 confirme cette tendance, avec une écrasante majorité des incidents concentrée dans les pays européens (80,9%).

Les pays candidats à l'adhésion à l'UE tels que le Monténégro et la Moldavie sont de plus en plus ciblés (passant de 0,7% des attaques au premier trimestre 2022 à 2,7% en

fin d'année 2022). La Pologne est toujours harcelée, avec un nombre record de 114 incidents liés au conflit en un an, tandis que les hacktivistes de guerre se concentrent particulièrement sur les pays baltes (157 incidents en Estonie, Lettonie, Lituanie) et les pays nordiques (95 incidents en Suède, Norvège, Danemark, Finlande). En comparaison, des pays tels que la France (14), le Royaume-Uni (18), l'Italie (14) et l'Espagne (4) sont davantage préservés.

Sur l'ensemble des cyberattaques enregistrées dans le monde pendant la période du conflit, 61 % de groupes d'hacktivistes pro-russes, dont Anonymous Russia, KillNet et Russian Hackers Teams occupent les premiers rangs. Ces groupes, apparus pendant le conflit, se sont organisés en réponse aux efforts des hacktivistes ukrainiens de l'IT Army au début du conflit. Ils sont plus structurés et utilisent des ressources de la cybercriminalité, organisées telles que le service de localisation de botnet Passion Botnet. Leur objectif est de harceler les pays qui justifient l'Ukraine. Les hacktivistes sont donc devenus une nouvelle composante du conflit, des groupes civils indépendants agissant avec des objectifs et des intérêts politiques précis, sans être directement sponsorisés par un État mais agissant par conviction. Ils proviennent de divers horizons et niveaux de compétence technique.

Au troisième trimestre 2022, une vague d'attaques DDoS a marqué un tournant, alors que le premier trimestre avait montré un paysage d'attaques très varié, avec des vols et des fuites de données, des attaques DDoS, de l'espionnage, de l'influence, des intrusions, des ransomwares, du phishing, des wipers et des info stealers sont presque également répartis. Les cyberattaquants utilisent principalement des attaques massives de déni de service (75%)

Je reprends la plume

Qui est Ivan Fontarensky ?

Ivan Fontarensky est directeur technique **Lutte Informatique Défensive** chez **THALES**. Il y a intégré et développé l'activité **Cyber Threat Intelligence**. Ivan a mené de nombreuses réponses à des incidents pour contrer des attaques avancées visant des organisations françaises.



Auparavant, il a travaillé chez Airbus en tant que responsable technique pour l'équipe de pentest et de réponses à incident. Il a également travaillé pendant plusieurs années au ministère de l'Intérieur en tant qu'expert informatique forensic et de mise au clair sur différents types de plateformes pour les autorités judiciaires.

THALES

Demande d'inscription pour le Lundi de la cybersécurité du mois de juin

Lundi 12 juin à partir de 18 h 00, en présentiel à l'université Paris Cité, 45 rue des Saints-Pères Paris 6^e, si le nombre des inscrits en présentiel le justifie, et toujours en parallèle en ligne par visio-conférence Zoom.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, les coordonnées de l'amphi de l'université Paris Cité, si vous avez demandé le présentiel, ou un hyperlien personnel vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements. **Et bien entendu, précisez si vous choisissez le présentiel ou le distanciel.**

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants.

Si vous souhaitez ne plus recevoir les lettres des « Lundi de la cybersécurité » mensuels, une simple demande par mail suffit. Si vous voulez être ajouté à la liste de distribution, demandez-le nous.

Quelques minutes avec « Les trophées de la femme cyber »

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une dizaine de minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'information. Le CEFCYS organise chaque année **les trophées de la femme cyber**. La présidente du CEFCYS, **Nacira Salvan** nous en parlera.

Voir pour les trophées de la femme cyber 2022 en :

<https://cyberwomenday-cefcys.com/>



Nacira Salvan est la présidente fondatrice du CEFCYS, docteure en informatique et experte en cybersécurité, elle a exercé pendant plus de 20 ans dans des postes à responsabilités de la sécurité de l'information. Elle a créé le CEFCYS pour encourager la diversité et la parité dans le secteur de la cybersécurité.



Le **CEFCYS**, **CE**rcl**es** **F**em**m**es de la **CY**ber **S**écurité, est une association qui vise à promouvoir et faire progresser la présence des femmes dans les métiers relatifs à la cybersécurité. Elles sont trop peu nombreuses aujourd'hui. Le CEFCYS organise et participe à des événements, des conférences, des programmes de mentorat et des publications sur la cybersécurité. Le CEFCYS compte plus de 400 adhérents.

<https://cefcys.fr/>

Lire le livre édité par le CEFCYS : *"Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité"*



Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements sur le web de l'ARCSI, en <https://www.arcsi.fr/>, pour les plus récents. Les événements plus anciens sont en https://www.arcsi.fr/evt_passes.php. Les enregistrements des organisations qui sont intervenues durant les « quelques minutes » se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui sont déjà intervenues dans nos « Lundi de la cybersécurité ». Cliquez sur un logo, vous obtenez l'enregistrement.

Nous remercions Francis Bruckmann, webmestre et membre du Conseil d'Administration de l'ARCSI pour son travail qui constitue la mémoire de nos événements.

Le coin coin de l'IA générative

Question posée au module d'Intelligence Artificielle générative inclus dans le moteur de recherche Bing, et sans livrer, bien sûr, de données confidentielles qui pourraient être exploitées :

Comment sont choisis les intervenants des « Lundi de la cybersécurité ? »

Réponse reçue : *D'après les résultats de la recherche web, les intervenants du Lundi de la cybersécurité sont des sommités dans divers domaines de la sécurité du numérique, choisis par Béatrice Laurent et Gérard Peliks, les organisateurs de l'événement. Ils présentent des sujets de pointe, en rapport avec la cybersécurité, devant un public de 150 à 200 participants. Les intervenants sont également soumis à une analyse des risques cyber pour garantir la qualité et la sécurité de leurs interventions.*



OK pour la qualification des intervenants et des sujets, mais soumettre les intervenants à une analyse des risques cyber ? L'idée ne nous était même pas venue, et ce n'est pas notre approche. 😊

Gérard

:

Nous faisons une pause en juillet / août

Le Lundi de la cybersécurité de septembre, le lundi 11 septembre (!) portera sur un sujet passionnant et très d'actualité autour de la cyber défense.

Notre intervenant le traitera avec brio.

